eduroam(UK) Policy

Document MF-POL-003 v.4

22/08/2012

Management Summary

Janet aims to foster collaboration between organisations whether publicly or privately funded that provide, support or collaborate in the delivery of education and research, and other public-sector organisations delivering public services, by facilitating roaming network access for members of such organisations. Provision of the federated eduroam service (the Service) is a major component in the fulfilment of this aim and is facilitated and governed in the UK by Janet through eduroam(UK).

This Policy outlines the requirements placed upon users of eduroam in the UK, the organisations issuing credentials (Home organisations), organisations providing network services (Visited organisations) and the operators of eduroam(UK) to ensure that each of these can be relied upon to play their part in ensuring the Service works effectively and securely. This is essential if the mutual trust required for the Service to function is to be maintained. **All users and providers of the Service are required to comply with the Policy on penalty of being barred from the Service.** Participating organisations must also ensure that their computing regulations enable individual members who breach this Policy to be subject to an appropriate disciplinary process *irrespective of their location at the time of the breach.*

The technical sanctions available to each service provider party are described below; these sanctions provide the ability to impose technical controls for the protection of the other parties and the Service against those who represent an immediate threat.

Introduction and Rationale

Allowing visitors and local users to obtain access to Janet using the same authentication mechanism and credentials regardless of location is the core function of eduroam and is to the mutual benefit of the whole education and research community.

Since participation is entirely voluntary, organisations will only provide the eduroam service if the benefits to them outweigh any problems that might arise from offering the Service. The continuing success of the initiative and further expansion and widening of availability of the Service therefore depends on co-operation and responsible behaviour from all participants; the aim being to ensure that organisations, particularly those offering a service for visitors, are not overburdened, disruption of the Service is avoided and that any problems that may arise are dealt with promptly and effectively.

This eduroam(UK) Policy has therefore been designed to meet the need for a policy which addresses these concerns and which must be accepted by all parties.

In addition to the above, visiting users should appreciate that their network access is a privilege, not a right, and must make best endeavours to abide by all policies that both home and visited organisations apply. It should be noted that each organisation has its own individual Acceptable Use Policy for its network to accommodate local technical or organisational concerns, and this may well result in different rules applying to the guest service provided by different organisations. Therefore visitors should normally read and accept the policies for each organisation whose eduroam services they use, wherever this is possible and the service-providing organisation can be identified, either before or early in their use of its network. (Visited organisations are required to make their local policies easily accessible, for example through their eduroam service information web page or their network access/device setup help page). In any case this eduroam(UK) Policy requires that visitors immediately cease any activity that they are informed breaches local policy.

The Policy

Users

- Are accountable to the organisations that issue them with their credentials (and to the law) for all use of such credentials and any activities undertaken with the authority of those credentials. In particular, users must not allow their own credentials, or network access authenticated by them, to be used by others. If the user believes that their credentials may have been compromised the user concerned must immediately report this to their home organisation;
- Must abide by restrictions applied by the home organisation and by Janet, including Acceptable Use Policies, Computing Regulations and Disciplinary Codes. Restrictions imposed by the visited organisations must also be respected. Where Regulations differ, the more restrictive applies;
- Must follow instructions provided by their home organisation to verify that they are connected to a genuine eduroam service providing adequate security before entering their login credentials;
- Must act immediately on requests by authorised staff of the visited or home organisation that relate to their use of the eduroam service.
- At the end of their association with their home organisation, must remove the eduroam profile from all devices that have been used to connect to the eduroam service and must not attempt to continue to use the service.

Home Organisations

- Are responsible to the community for the good behaviour of users they authenticate;
- Must enforce this eduroam(UK) Policy in relation to users they authenticate and investigate security breaches affecting their accounts, if appropriate informing any visited organisations that may be affected;
- Must promptly disable, at least with respect to eduroam, accounts of users who no longer have a primary association with the organisation;
- Must make their users aware of roaming conditions, including Computing Regulations and Acceptable Use Policies;
- Must educate their users about how to follow best security practices when using the Service, including how to identify a genuine eduroam service;
- Must provide support for their users when roaming elsewhere (as a minimum, web-based information should be provided);

- Must provide eduroam(UK) with up-to-date contact details and act promptly on reasonable requests from eduroam(UK);
- Must inform Janet CSIRT promptly of any apparent breaches of security affecting the privacy of user credentials.

Visited Organisations

- Must ensure that systems that support visiting users are configured, maintained and operated securely, so as not to put the security of other organisations or their users at risk;
- Must make their own AUP readily available to roaming users;
- Must assist home organisations in supporting their roaming users when required, though the home organisation must take primary responsibility;
- Must provide visiting users with sufficient information to identify the eduroam services they provide (for example locations covered, service level, SSIDs)
- Must keep sufficient logs to be able to trace provision of eduroam connection/Internet access (but not what the specific Internet activity was) to an authenticated user's device and if available, user identity, and keep these logs securely for a minimum of three months;
- If activity logs are collected (e.g. on a web proxy), must make the relevant portions available to home organisation and/or Janet Roaming when these are required to investigate misuse;
- Must accept and log complaints of misuse and forward these promptly to the appropriate home organisation;
- Must provide eduroam(UK) with up-to-date contact details and act promptly on reasonable requests from eduroam(UK);
- Must inform Janet CSIRT of any apparent breaches of security affecting the privacy of user credentials.

Janet eduroam(UK)

- Must protect the security of participating organisations and systems by implementing best practice;
- May exceptionally reduce or remove service without notice when this appears necessary for operational or security reasons;
- Must record authentication attempts and outcome (if possible) and retain these records securely for a minimum of three months and a maximum of six months;
- Must provide relevant extracts of this record to the home organisation or Janet CSIRT when requested to do so;
- Must inform Janet CSIRT promptly of any apparent breaches of security affecting the privacy of user credentials.

Technical Sanctions

As noted below, the design of the Service in the UK gives each party the ability to impose technical controls to protect themselves and the Service against those who represent an immediate threat. However, as the effectiveness of the Service relies on co-operation, such technical measures should be regarded as a temporary solution until the problem can be resolved. Possible technical controls include the following:

- eduroam(UK) may suspend an organisation's ability to participate in the Service, either as a home or visited organisation, for failure to uphold this Policy, as for the Janet Acceptable Use and Security Policies;
- Visited organisations may prevent use of their networks by all users from a particular home organisation by configuring their RADIUS proxy to reject that realm and their access points to re-authenticate users currently connected; in some cases a visited organisation may also be able to block a single visiting user, but this depends on the particular technology used. In both cases, visited organisations must inform eduroam(UK) of such measures.
- Home organisations may withdraw an individual user's ability to use the Service by configuring their own RADIUS server.

If a technical sanction is imposed that affects other organisations this must be reported immediately to eduroam(UK), which will endeavour to assist the organisations concerned to resolve the problem, allowing the full Service to be restored. If a technical sanction involves a particular home organisation then the visited organisation should inform that home organisation as a matter of courtesy.